

Pride of Place

Author(s): David V. Gioe, Margaret Smith, Joe Littell and Jessica Dawson

Source: *PRISM*, 2021, Vol. 9, No. 3 (2021), pp. 140-157

Published by: Institute for National Strategic Security, National Defense University

Stable URL: <https://www.jstor.org/stable/10.2307/48640751>

## REFERENCES

Linked references are available on JSTOR for this article:

[https://www.jstor.org/stable/10.2307/48640751?seq=1&cid=pdf-reference#references\\_tab\\_contents](https://www.jstor.org/stable/10.2307/48640751?seq=1&cid=pdf-reference#references_tab_contents)

You may need to log in to JSTOR to access the linked references.

---

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at <https://about.jstor.org/terms>



Institute for National Strategic Security, National Defense University is collaborating with JSTOR to digitize, preserve and extend access to *PRISM*

JSTOR



Insurrection at the U.S. Capitol: QAnon Shaman, Jake Angeli" (Johnny Silvercloud At Shutterstock)

# Pride of Place

## Reconceptualizing Disinformation as the United States' Greatest National Security Challenge

By David V. Gioe, Margaret Smith, Joe Littell, and Jessica Dawson

**O**n January 6, 2021, long held assumptions about the meaning of American national security were challenged when insurrectionists stormed the United States Capitol, attempting to overturn the results of the 2020 Presidential election. Largely fueled by a toxic combination of mis- and disinformation about American democratic institutions, processes, and elections, the insurrection highlights how misguided mob power—energized by false information—can have devastating results. Interestingly, the attackers were not social outliers and recent polls indicate that nearly 20 percent of Americans approved of the insurrection.<sup>1</sup> What the attack on the Capitol suggests, is that America's civil society is struggling to function. Social norms are being challenged and morphed by the current contested information environment, which poses an urgent and existential threat to democracy—namely, a declining respect for government and institutional norms, a diminishing trust in foundational democratic processes, and a growing aversion to the rule of law. In the contested information environment, both domestic and foreign actors use mis- and disinformation for malign and malicious purposes and, if left unchecked, the information environment presents adversaries with an attack surface that conventional national security measures fail to secure.<sup>2</sup> Ultimately, the speed and scale at which mis- and disinformation penetrate and disrupt civil society is America's most urgent national security challenge.

Surprisingly, “fake news” only entered the American lexicon in 2016,<sup>3</sup> but mis- and disinformation—and America's increasing receptivity to it<sup>4</sup>—have been eroding American democratic norms for decades.<sup>5,6</sup> Mis- and disinformation generate domestic chaos by championing falsehoods couched in seemingly legitimate sources of information designed to chip away at social cleavages. Additionally, mis- and disinformation undermine public trust in democratic institutions, denigrating public esteem in science, journalism, higher education, and health systems, among others. Yet, the domestic strife resulting from foreign and domestic mis- and disinformation campaigns was not identified as a threat in any U.S. national security strategy until very recently.

---

All authors are researchers affiliated with the Army Cyber Institute at West Point. Additionally, David V. Gioe is Visiting Professor of Intelligence and International Security in the Department of War Studies at King's College London. Jessica Dawson is a sociologist who focuses on extremism, morality, narratives, and social change that comes from the digital disruption of social processes. Joe Littell is a U.S. Army officer and graduate of Duke University, and Margaret Smith is a U.S. Army officer and assistant professor in the West Point department of social sciences. This analysis is solely that of the authors and does not reflect any official position of the U.S. Military Academy, the Department of Defense or the United States Government.

This article is written in response to the Capitol insurrection and is motivated by the thesis that democracy cannot exist without a shared reality. Additionally, threats to a nation-state's shared reality are threats to the state's continued existence and should be prioritized accordingly. We argue that the national security concerns resulting from mis- and disinformation mandate a coordinated and well-resourced government response. In the following sections we first address the development of mis- and disinformation to identify the roots of the current crisis. We then explain why the threat from mis- and disinformation represents a national security crisis, and finally, we identify potential solutions to mitigate mis- and disinformation's ability to deepen societal divisions in America. Potential policy solutions include increasing awareness and attention from national security leaders, raising public concern about the deleterious effects of mis- and disinformation, and fostering a proactive and educated public to assist in curbing the spread of mis- and disinformation.

## The Curious Absence of Disinformation in U.S. National Security Strategies

The first National Security Strategy of the George W. Bush Administration contains a striking omission: the document fails to mention the threat of mis- or disinformation.<sup>7</sup> President Bush's second National Security Strategy suffers from the same oversight and only briefly discusses threats emanating from "sub-cultures of conspiracy and misinformation"<sup>8</sup> in the context of Salafi jihadism. "Terrorists," the Bush Administration explains,

recruit more effectively from populations whose information about the world is contaminated by falsehoods and corrupted by conspiracy theories. The distortions keep alive grievances and filter out facts that

would challenge popular prejudices and self-serving propaganda.<sup>9</sup>

Yet, over the past decade, it is increasingly apparent that mis- and disinformation, and the security threats they pose, are not limited to the likes of al-Qaeda, the Islamic State, or fringe conspiracy groups.

Making only minor improvements to the Bush Administration's strategy, the Barack Obama Administration included a passing reference to "Moscow's deceptive propaganda" on page 25, of a 29-page document.<sup>10</sup> It was not until the Donald Trump Administration that mis- and disinformation were given more attention, noting that "America's competitors weaponize information [and] disseminate misinformation and propaganda."<sup>11</sup> Striking a markedly different tone than previous administrations, the Trump White House determined the threat was not from divergent and disparate terrorist groups, but instead from "America's competitors," elevating the threat from nonstate actors to state-supported activities.

Despite their destructiveness, mis- and disinformation campaigns have failed to garner much attention from the national security community. Naturally, every administration's National Security Strategy reprioritizes all security threats based on the current operational context and their governing agenda. But, even the most recent strategies have fallen short by failing to identify the domestic and foreign variants of mis- and disinformation as a primary national security threat. To be precise, the threat is not the malign information, but is instead the American public's inability to manage and mitigate mis- and disinformation that poses the urgent threat. The effect is an undermining of America's shared reality and a fracturing of the framework through which Americans understand global developments as well as domestic issues.

The Joe Biden Administration has an opportunity to remedy past national security oversights by

including a robust discussion of threats from mis- and disinformation as it crafts its own National Security Strategy. The Biden Administration claims, “this moment is an inflection point,” and we agree, believing that a shared reality is necessary for membership in the community of values that defines America. America cannot act with unity or purpose, globally or domestically, if it is a “house divided” against itself, to borrow Abraham Lincoln’s famous metaphor.

In early March 2021, President Biden released an Interim National Security Strategic Guidance, outlining the administration’s security posture as a final version is produced.<sup>12</sup> Promisingly, disinformation is covered in detail as a threat to American and global democracy:

Anti-democratic forces use misinformation, disinformation, and weaponized corruption to exploit perceived weaknesses and sow division within and among free nations, erode existing international rules, and promote alternative models of authoritarian governance.<sup>13</sup>

Unlike past administrations, the interim guidance clearly identifies disinformation as a threat and insists that if global democratic values are to survive, America must regain the trust of its allies and rejuvenate the public’s trust in its domestic institutions. However, despite outlining the threat of disinformation and the dangers posed by it, the interim guidance does not discuss mitigation efforts as prescriptive and substantive policy solutions are not included in the report. We therefore see this article as an opportunity to contribute in a specific manner toward crafting a forthcoming Biden administration National Security Strategy document that contains a strategy to appropriately deal with mis- and disinformation.

## Reimagining and Reordering Threats

Because the Biden Administration has emphasized that it wishes to chart a new course in national

security, we propose an update to how national security challenges are imagined and defined. Our reimagining will undoubtedly make America’s national security apparatus uncomfortable but, throughout history, technological advancements and innovations have changed the character of warfare with corresponding re-conceptions of threat, purpose, and national defense. Examples include heavy armored vehicles, air power, nuclear technology, the internet, and militarized space to name but a few. Despite hiccups in implementation, American doctrine and theory have routinely adapted to account for substantial changes in technology, adversary competence, and intent. We therefore argue that acknowledging the widespread and hostile dissemination of disinformation as a top national security concern—and adjusting the U.S. national security posture to reflect the change—is necessary and achievable in the near term.

Unlike other security threats, mis- and disinformation are an epistemic threat—a threat to what people believe is *real*. Knowledge should be understood not as an individual attribute but rather, as “socially distributed.”<sup>14</sup> Over the last forty years, the civic institutions that help define what is real and what is true have been steadily eroded,<sup>15</sup> giving malign actors a vector to distort and undermine the American public’s shared reality. For the purposes of this article, we endorse the articulation of “shared reality” described by Gerald Echterhoff and E. Troy Higgins:

the experience of having in common with others inner states about the world. Inner states include the perceived relevance of something, as well as feelings, beliefs, or evaluations of something. The experience of having such inner states in common with others fosters the perceived truth of those inner states.<sup>16</sup>

Humans are motivated to create shared realities because they establish a grounding truth about



the world around us. Religious affiliations are a good example: shared beliefs create a rooted sense of identity among a congregation and a common way of understanding the world and explaining its mysteries. By developing shared realities, Echterhoff and Higgins claim, people can fulfill a basic need by establishing valid beliefs about the world. People with a shared reality are bound by common values and a common understanding of the world and their place in it. As a result, shared realities enable people to interpret events and underlying facts in a similar manner or from a common place of understanding. To extend the claim, we argue that a common construct underpins the way a polity interacts with—and acts within—a nation-state. To continue the parallel with organized religion, many church denominations have splintered through divergent understandings of Biblical teachings. In the same way, societies can also fracture along lines of interpreted reality.

The most recent example of fissures to an American shared reality is the January 6

insurrection. As the mob breached the Capitol, it became clear that Americans do not live in a common, fact-based, shared reality. Perhaps more controversial than acknowledging that Americans are not rooted in a shared reality, is our assessment that the public's appetite for confirmational and explanatory disinformation over fact-based sources far exceeds the conventional national security threats, like belligerent foreign powers, nuclear proliferation, and Salafi-jihadist terrorism. Without a shared reality, truth becomes negotiable, existing on a spectrum and leaving a confused and agitated American public without a common understanding of current events. After January 6, and despite the negative impact of leaving Washington D.C. in an extended military lockdown, many leaders agreed that mis- and disinformation surrounding the election, voting systems, and the Biden administration's legitimacy mandated the deployment of over 20,000 National Guard troops to safeguard the Capital. The United



Voter Fraud' rally marches to Supreme Court in support of Donald Trump, who refused to concede election.  
(Bob Korn at Shutterstock: 186799326)

States has not experienced a similar domestic security posture since the days immediately following the September 11, 2001 (9/11) attacks.

The American military response to 9/11 also provides a useful foil in the disinformation fight. During the Cold War, “hard” applications of conventional military power (and their deterrent effect) were enough to maintain the superpower standoff. In contrast, the disinformation challenge has more in common with terrorism or climate change because the root problems are complex and applications of conventional power are ill-suited to manage the problem, much less claim a victorious end-state. In this case, America’s formidable military might has little application to countering false and misleading narratives, but the Pentagon has been slow to apprehend this development. Unlike the Cold War, the response to mis- and disinformation must include a “whole of society” approach, as we will explore in greater detail after a brief overview of America’s historically skeptical relationship to centralized authority and an identification of how foreign actors have sought to exploit this inherently American trait.

## Evolution of a Disinformation-Driven Security Crisis

Nearly two hundred years ago, sociologist Harriette Martineau argued that America had done the impossible: it had demonstrated that self-rule was possible.<sup>17</sup> Contrary to oversimplified accounts of early American harmony, Martineau’s investigation of society in America in the first post-Revolution generation also underscores how democracy in America has always been contested and shaped by public debate. Martineau would have recognized many of contemporary America’s political traditions in which elected officials routinely apply a partisan spin to social issue framing, leading to disparate narratives, confusion over facts, and two distinct shared realities based on political persuasion.

Of course, different viewpoints and perspectives have always existed to some degree; indeed, these are the basis of political ideologies and parties, but Reuben E. Brigety II argues that the 2020 presidential campaign may have been a watershed tipping point because it exposed societal cleavages and how party identity is linked to a foundational identity, like race or religion.<sup>18</sup> Moreover, when foundational identities become the organizing principle of a country’s political life, tribal conflict becomes more likely. Brigety emphasizes that “the [2020] campaign looked less like a contest of ideas and more like a battle between tribes, with voters racing to their partisan corners based on identity, not concerns about policy.”<sup>19</sup>

While American political parties have long-running stereotypes associated with their respective constituents, party affiliation was heretofore less public and more private, leaving people more inclined to build communities and friendships based on more robust, less divisive civic identities unattached to politics. As these diffuse civic organizations have declined over the last 40 years,<sup>20</sup> they combined with neighborhood sorting that moved Americans into more and more homogeneous neighborhoods,<sup>21</sup> perhaps a proto-filter bubble presaging the type of sorting done by and through social media. As we will explore, filter bubbles and echo-chambers threaten shared reality, which we identify as a prerequisite for productive policy deliberation. When this common operating picture becomes unrecognizable to a large number of voters, it is almost foreordained that civil chaos should follow. America’s culture wars, coupled with declining trust in American institutions, have helped harden the ideological and foundational identities affixed to political parties. If things become brittle once hardened, the trajectory of such tribalism in American political and civic life is alarming, and the canaries are already in the coalmine.

For those paying attention to the steady erosion of confidence in American norms and institutions

over the past few decades, the events of January 6 did not come as a surprise. For several years, a systematic influence campaign aimed at undermining public trust has occurred, directed at institutions like the courts, elections, and the broader mechanisms inherent to democracy, although the erosion of trust and the January 6 attack on the U.S. Capitol was *not* solely caused by conspiratorial fiction about democratic institutions spread via mis- and disinformation campaigns. Some of the recent decline in public trust is warranted and expected, as societal norms have changed in response to increasing access to information and rapid globalization brought about by the internet. In fact, some antecedents to January 6 are *real* events and *real* public concerns, but influencers, media personalities, and charlatans have taken fact-based threads and twisted them together with falsehoods, weaving tales and drawing connections between stories and events to create a pseudo-reality that no longer resembles the facts, but instead supports their specific political and social agendas. We now provide a brief historical overview to illuminate the conspiratorial threads that, when woven together, help explain the troubling events at the Capitol.

Distrusting government is not new and the experiences of the past two generations justify a healthy criticism of government and raise the legitimate question of whether the government is worthy of the public's trust. The Watergate scandal, the Pentagon Papers, and the Vietnam War all tested public trust in government. Those examples left the Baby Boomer generation with a lingering skepticism of their leaders and institutions. Trust has not improved in younger generations because of the September 11, 2001, attacks and the "forever wars" in Iraq and Afghanistan. Operation Iraqi Freedom began with an intelligence failure and nearly every official who used the word "progress" to describe America's ongoing presence in Afghanistan was being dishonest with the American people.<sup>22</sup> Ultimately, the already low trust in government created a fertile field for conspiracy

theories crafted from mis- and disinformation to take root. Mis- and disinformation do not circulate in isolated information systems – instead, they intersect with, and shape, society's natural information flow guided by social media. Into that complex ecosystem entered the Russians.

## Enter the Russians

In 2015, conspiracies about Jade Helm, a routine military training exercise that takes place across Texas and the greater American west, rose to prominence on social media, bringing previously fringe ideas to the news feeds of a large, mainstream audience.<sup>23</sup> Russian cyber actors, mimicking American social media users online, propagated radical theories about Jade Helm, claiming that the military exercise was really being used by the Obama Administration as a ruse to round up its political opponents.<sup>24</sup> Analysis of the Jade Helm conspiracy tends to focus on the success of the Russian influence and how the campaign even led the Texas Governor to publicly question the true purpose of the training exercise. However, less emphasized is the strain of deep-seeded anti-government sentiment that the Jade Helm conspiracy reveals, and it justifies the Russian approach in that vein.<sup>25</sup> Legitimate concerns about armed government overreach at incidents like Ruby Ridge, Idaho, in 1993 and Waco, Texas, in 1994 fed into the suspicion fueling the anti-government militia movement.<sup>26</sup> These fringe concerns about the military exercise entered the mainstream political sphere as politicians sought to capitalize on the public's outrage for political advantage.<sup>27</sup> Such distortions from reality provided fertile soil for a Russian disinformation campaign.

If the 2015 Jade Helm exercise was a proof of concept for Russian meddling via social media, operating in the American information environment became a full scope operation by 2016. Even though most Americans likely became aware of Russian influence operations following documented



Russian interference in the 2016 presidential election,<sup>28</sup> Russia has meddled in U.S. media and social narratives for decades before the advent of social media.<sup>29</sup> The legacy of Russian interference dates back to the fall of tsarist Russia and was a hallmark of the Cold War, and we can credit Russia, China and other foreign actors (all adept at information operations) with exposing how vulnerable American society is to mis- and disinformation and, more importantly, how inept Americans are at mitigating it. The Russians did not create American suspicion of the federal government but, the Russian influence campaign surrounding Jade Helm skewed, weaponized, and amplified long-standing American narratives, harkening back to President Ronald Reagan's claim that "government is the problem,"<sup>30</sup> twisting a conservative skepticism of government overreach into outright distrust. To make matters worse, as the Jade Helm conspiracy gained

momentum, it was not quashed but was instead humored by Texas state officials, giving the conspiracies and false narratives an air of legitimacy.<sup>31</sup>

It is hard to overstate this fork in the road for the Russian approach to American audiences.<sup>32</sup> Russia's Jade Helm-related active measures worked, and the ease with which the Jade Helm disinformation campaign took over the mainstream narrative proved just how easily the American public could be swayed via digital means, ultimately paving the way for Russia's (and others') digital influence activities during the 2016 election and beyond.<sup>33</sup>

### Foreign Disinformation Flourishes Amid Domestic Social Discontent Amplified by Social Media

It is critical to note that foreign adversary influence operations have not created nor invented the schisms in American society; instead, they identify,



Facebook launches PR campaign as public backlash after Cambridge Analytica scandal and Russian interference in 2016 elections. (NYCStock)

exploit, and exacerbate them. Domestically generated discontent is what brought protestors to the Capitol on January 6 and the most extreme of them arrived with pipe bombs, zip ties for handcuffing hostages, and calls for executions.<sup>34</sup> This is a rich environment for foreign and domestic malevolent actors to ply their trade. In a sense, even if the seeds are foreign, the fertile field is American, and this blurring of the lines between foreign and domestic disinformation leaves American national security mandarins and agencies in uncomfortable territory in terms of legal authorities, lanes of the road, and responsibilities for combatting a polluted information environment that does not recognize national boundaries.

Above we identified factors like the erosion of trust in government that make citizens more receptive to mis- and disinformation. According to multiple academic studies, one in four Americans believes in at least one conspiracy theory, and, perhaps unsurprisingly, belief in one is strongly predictive of belief in other conspiracies.<sup>35</sup> Research also shows that conspiracy theories are often partisan and that one of the strongest predictors of a person's receptivity to specific conspiratorial ideas is their political orientation.<sup>36</sup> On January 6, the attacking mob was joined in spirit by millions of Americans watching from home, representing a variety of backgrounds, and spread across social strata. Many passive supporters agreed with the mob and had also lost trust in the American government, believing oft-repeated claims of a stolen election.<sup>37</sup> Based on the close 2020 election and scholarly evidence linking political affiliation to a person's susceptibility to specific conspiratorial narratives that align with their political beliefs, America's lack of a shared reality for electoral outcomes is hardly surprising—realities diverge as partisan polarization increases.<sup>38</sup> Tying several strands together, a recent Pew survey found striking differences along party lines regarding the impact of the COVID-19 pandemic, election legitimacy, willingness to accept the vaccines, and other

critical elements necessary to coexist in society.<sup>39</sup> It seems clear that diverging shared realities appear to be largely driven by partisan politics, and it is therefore understandable that foreign influence operations would wish to join domestic actors and focus their attention on that civically-vulnerable area.

Just as deceitful government activity such as Watergate or hyped up intelligence over the justification for the Iraq war seemed to justify or warrant popular skepticism, the most successful mis- and disinformation campaigns are often rooted in fact or closely mimic actual events. Most of the public reacted in horror to the 2016 “Pizzagate” tragedy, when a man traveled from his home in North Carolina to Washington, D.C., and fired a rifle into a pizza restaurant. The man was there to investigate the alt-right (loosely connected online white supremacist groups) claim that the pizza restaurant was really a cover for a child sex-trafficking ring run by wealthy and socially well-connected Americans. On the surface, the claim sounds ridiculous, but not long after the pizza parlor shooting, wealthy socialites, Jeffrey Epstein and Ghislaine Maxwell<sup>40</sup> were charged with a similar crime, leading many to believe the alt-right was correct in its suspicions. The “Pizzagate” event highlights how extreme narratives are often validated by actual events and how conspiracy theories are often underwritten by historical events or prior incidents.<sup>41</sup>

## Digital Technology and Social Media Amplify and Enable Foreign Disinformation Operations

The social media ecosystem has expanded and accelerated the propagation of mis- and disinformation.<sup>42</sup> Acting like a megaphone, social media has incited violence and allowed foreign trolls, domestic politicians, cable news hosts and other influencers to spread falsehoods, place blame, and target opposition groups. While conspiracy theories and alternative realities have long histories,

digital information technology—particularly social media—has enabled their spread, allowed believers to easily connect, and developed a cadre of vocal leaders to coordinate attacks in virtual and physical spaces.<sup>43</sup> The mix of legitimate grievances, mis- and disinformation, and unchecked social media algorithmic amplification is both driving and providing the soil for this national security crisis.<sup>44</sup>

Various geopolitical adversaries have identified this gap in the U.S. national security posture and have begun exploiting it, even down to the local level where hostile foreign actors have sought to exacerbate American suspicions about electoral integrity. For instance, the past few American elections have seen the increasingly populous state of Florida act as a swing state with each political party competing doggedly for every vote. In October 2020, weeks before the November election, many Floridians received menacing emails from an address associated with alt-right group, the “Proud Boys,” threatening harm if they did not vote for President Donald Trump and change their voter registration to Republican. Proud Boys leadership denied any involvement and U.S. authorities were hasty to pin the blame on Iranian actors using overseas servers to spoof Proud Boys emails. U.S. intelligence officials also noted a video, apparently sponsored by Iran, that suggested ways to fraudulently cast ballots.<sup>45</sup>

These efforts at stoking voter skepticism were predicted in advance as early as August 2020 by the U.S. National Counterintelligence and Security Center, which issued an assessment that “Iran seeks to undermine U.S. democratic institutions, President Trump, and to divide the country in advance of the 2020 elections.” Further, “[their efforts] probably will focus on online influence, such as spreading disinformation on social media and recirculating anti-U.S. content.”<sup>46</sup> It seems reasonable that Iran would choose to act to undermine voter confidence when leading American politicians were preemptively doing the same thing.

Iran, however, was far from the only foreign actor to appreciate the vulnerable American attack surface.

If Iran’s rather ham-handed approach to election meddling seemed opportunistic, Russia’s concept of Hybrid Warfare<sup>47</sup> and Chinese Three Warfares<sup>48</sup> have thoughtfully considered the power of influence operations at the strategic level, and, in turn, have drastically restructured their vision for how malevolent influence operations against the United States should be conducted. Both strategic approaches subordinate conventional kinetic warfare to overarching information campaigns, drastically reducing U.S. military capabilities to intervene or muster the political will to contest the outcome.

Russian actions within the Ukraine mirrored similar operations domestically in the United States. Sowing distrust and instability<sup>49</sup> within a region allows for a contested information environment in which further disinformation campaigns can thrive. Russian forces regularly harassed and attacked racial minorities such as the Roma, Jews, and Hungarians within Crimea, attempting to blame the actions on Ukrainian forces.<sup>50</sup> Direct harassment and psychological warfare was conducted against Ukrainian soldiers on the front lines through phone calls and text messages to them and their families to torment them.<sup>51</sup> This closely mirrors efforts by Russia in the United States to cause racial division amongst African Americans and the population at large, playing to both pro- and anti-police narratives.<sup>52</sup> Russia furthermore pushes transnational white supremacist extremism in both the United States and Russia.<sup>53</sup> Numerous controversial American white supremacists like David Duke and Richard Spencer have praised Russia for their efforts in promoting white supremacy.<sup>54</sup> Spencer’s ties run even deeper, as he was married to Nina Kouprianova,<sup>55</sup> a Russian national, long-time adherent of Russian nationalist icon Aleksander Dugin,<sup>56</sup> and Kremlin mouthpiece.

China’s efforts have also ramped up to exploit vulnerable flanks in East Asia and beyond.

Previously these methods were predominately focused on regional adversaries, such as Taiwan or Vietnam,<sup>57</sup> and China's maritime ambition for complete control over the South China Sea. Operations utilized a myriad of approaches to include aggressive seaborne expansion and fortification, use of ambiguous naval militias, and use of non-internationally recognized maps of territorial waters to sway the narrative.<sup>58</sup> More ambitious Chinese efforts included informational forays against academia,<sup>59</sup> professional sports,<sup>60</sup> and Hollywood.<sup>61</sup> Chinese academic espionage resulted in numerous arrests in 2020 and the investigation of 189 more grant recipients, 54 of which had undisclosed foreign ties to China.<sup>62</sup> Both the NBA,<sup>63</sup> and American video game developer Blizzard-Activision<sup>64</sup> found themselves censoring employees in response to anti-democratic crackdowns in Hong Kong, showing further how China can influence large numbers of Americans through its leverage of multinational corporations. Chinese media markets are heavily regulated by the government, requiring all Western movies entering the market to show China in a positive light.<sup>65</sup> Considering Hollywood's reach into the American movie goer audience, many citizens only know of China through its portrayal in films, thus muddying the waters. Increasingly, following the global COVID-19 pandemic, China has shifted heavily into online social media channels, particularly anglophone ones to contest the narrative that it was to blame for the outbreak and insufficient initial response. To argue in favor of its role in combating the pandemic China has attempted to discredit U.S. and other Western democratic responses, as well as shift their culpability in the outbreak's origins.<sup>66</sup>

## Solutions for Malign Digital Interference

As the above sections illustrate, the threat is urgent, complex, and non-traditional. Any whole-of-nation response to malign manipulation of the information environment requires both

government and private sector responses, cooperative public-private partnerships, and tasks and responsibilities down to the level of the individual citizen. The balance of this article will explore some necessary steps and adjustments toward addressing the disinformation threat.

Technical responses are often the first ones proposed when addressing digital threats, yet consensus on a technical response has yet to emerge. As Jon Bateman and Craig Newmark have complained, "Social media disinformation discussions are going in circles."<sup>67</sup> Currently many filtering algorithms and methodologies are being tested by large social media platforms. Twitter has attempted to use warnings and forms of soft moderation surrounding COVID-19 and the results of the 2020 U.S. Presidential election,<sup>68</sup> with varying results.<sup>69</sup> Other platforms, such as Reddit, have attempted to de-platform individuals and groups in order to meet the same ends.<sup>70</sup> Often these de-platforming methods have merely slowed the movement of information temporarily, as users migrate to more salient platforms.<sup>71</sup> However, many argue that such filters encroach on First Amendment rights and limit user capacity to practice thinking critically about the information they ingest.<sup>72</sup> This has caused a schism politically where platforms like Voat, Gab, and Parler, among others, have marketed themselves as platforms of free speech.<sup>73</sup>

These methods are reactive and do not account for emergent technologies such as generative adversarial networks, or GANs, algorithmic confounding, and data poisoning. GANs have already gained traction through their use in Deepfakes,<sup>74</sup> a technology so democratized that a mother in Pennsylvania used it against her daughter's teenage rivals.<sup>75</sup> Algorithmic confounding and data poisoning can be used to circumvent previously mentioned attempts at filtering, forcing additional users to see false or misleading content at a greater rate than typical of an average user.



However, most recommendation engines and content filtering technologies actually push users to more extreme viewpoints by surrounding them with media and content that reaffirms prior beliefs, reinforces already formed opinions, and connects them to similarly extreme users.<sup>76</sup> For example, 64 percent of Facebook users who join extremist groups do so because of algorithmic recommendations.<sup>77</sup> Essentially, filtering algorithms create echo chambers that normalize radical ideas and extreme opinions, amplifying bias and dangerous behaviors,<sup>78</sup> working within existing societal schisms, offering justifications for existing fears or prejudices.<sup>79</sup> For example, research from the University of Warwick demonstrates a correlation between increased Facebook usage and violence against immigrants.<sup>80</sup>

Social media has many benefits, such as playing a critical role in keeping socially distant loved ones connected during the COVID-19 lockdown, but the filtering of society into isolated media and content bubbles has created multiple shared realities instead of unifying citizens under a single shared reality. If social media is hard to police, it is also still largely unfiltered, allowing prominent voices, however extreme, to spread mis- and disinformation.<sup>81</sup> The result is a far more complicated world, with multiple realities existing in an information nightmare that is difficult to dissect, understand, or combat.<sup>82</sup>

The terms “alternative facts” and “fake news” became popular vernacular in the “post-truth” era of the Trump Administration, but these are just the newest iterations of mis- and disinformation tactics.<sup>83</sup> What is different today is how social media platforms and technology amplify the problem to a scale without historical precedent.<sup>84</sup> Winston Churchill’s quip, “a lie is half-way around the world before the truth has a chance to put its pants on,” is now woefully outdated as recent studies confirm that mis- and disinformation travel, on average, 6 times faster than fact.<sup>85</sup> As algorithms are designed for amplification of engagement, verified truth

and legitimate news sources do not stand a chance against computational propaganda.<sup>86</sup> Yet there are promising developments. NewsGuard, for example, is a technology popularized when Microsoft implemented it into its Edge browser, that gives trust ratings to users as they browse websites.

To mitigate the risks associated with mis- and disinformation, America should reintroduce civic education into elementary education and, continue it through a child’s entire academic career to grow a robust, active, and engaged public. Civic engagement is an investment in democracy and students need to understand how their involvement is critical to the health of their country. Modern civic education should be directed towards media and information consumption to help raise a public capable of coping with a saturated information environment flush with mis- and disinformation. Curricula should encourage active engagement with trusted media sources, teaching students to tease out facts, identify bias, and draw informed conclusions. Finland provides a good example and currently leads the world in digital media education,<sup>87</sup> scoring among the very highest of countries in indices relating to the strength of its democracy<sup>88</sup> and the digital literacy of its population.<sup>89</sup> With targeted civic education aimed at civic institutional knowledge and digital literacy, America can build a more robust society that is less susceptible to mis- and disinformation.

Educational efforts must also encourage students to engage in civil discourse with people who have conflicting opinions. One effort, Millions of Conversations,<sup>90</sup> is a civic campaign founded by Samar Ali, a former White House Fellow and attorney. Ali’s initiative encourages dialogue across parties, fostering conversation with the intent of healing social divisions. The effort encourages people to non-judgmentally exchange narratives—an activity that Joshua L. Kalla and David E. Broockman recently found can reduce exclusionary attitudes. Kalla and Broockman

conducted three experiments targeting exclusionary attitudes towards unauthorized immigrants and transgender people. They found that dialogue and interpersonal exchanges reduced exclusionary attitudes towards the marginalized out-groups. However, the key to Millions of Conversations and Kalla and Broockman's study is the *exchange* of narratives—one-sided, face-to-face conversations that deliver arguments produced no effect on exclusionary attitudes. To reinforce good civic behavior, America's leaders must set the example and reach across the aisle, giving citizens behavior to emulate. Leaders across the country should establish forums for narrative exchanges and encourage more grass-roots organizations like Millions of Conversations.

Additionally, elected officials should counter mis- and disinformation publicly, acting as a whistle-blower when they identify false narratives and as educator when they publicly correct a false or misleading story. Government agencies must get involved too—like the Cybersecurity and Infrastructure Security Agency (CISA), which took proactive steps—even developing the hashtag #protect2020 to support its campaign—to dispel election rumors by setting up a public website<sup>91</sup> to debunk popular myths about voting security and fraud. In a democracy, retribution for correcting falsehoods is dangerous and will discourage shared understanding—as when former CISA Director Christopher Krebs was fired<sup>92</sup> for coming out publicly against claims that the 2020 election was rigged. Because elected officials are beholden to the public, debate and civil discourse among citizens is critical to democracy.

Another cornerstone of digital literacy is the ability to detect false and misleading information—education, as discussed above, can grow a public less susceptible to conspiratorial thinking. However, simple detection is not enough, and detecting and removing mis- and disinformation on social media,

at speed and scale, is not easy. Social media platforms are currently drawing their own lines between legitimate and illegitimate online speech with the help of sophisticated yet non-transparent detection algorithms and extensive human involvement. It is impossible to catch and verify all false and misleading information, but the U.S. government should consider mandating greater transparency surrounding what content is moderated by private social media companies.

Additionally, social media firms should be held accountable on several fronts, most notably being how quickly they respond to fraudulent accounts, how thoroughly they respond to government oversight requests, how transparent they are with data usage and privacy policies, and the transparency of their content filtering mechanisms. Government regulation may be required, but ultimately, technology companies cannot solve the mis- and disinformation crisis and it remains the responsibility of every citizen to engage in critical thinking and try to distinguish between news and “fake” news.

Yet, despite being the responsibility of every citizen to educate themselves on the threat of mis- and disinformation, the erosion of a shared reality makes people across all social strata<sup>93</sup> highly susceptible to mis- and disinformation or “fake” news. Interventions that target information nodes, like public figures with large social media followings or message board moderators, can influence previously isolated sectors of the internet. In a local or closed network, small amounts of information are shared and constantly reinforced by group members. Exacerbating the cycle of a closed information loop are social media and search engine algorithms. Injecting additional and diverse information sources into insular online communities may challenge the group's ideological status quo.

A team of researchers recently demonstrated that professional norms in journalism like fact checking, published corrections, and retractions

work to insulate people from conspiratorial thinking by providing oversight and reducing the incentive to print whatever will go viral.<sup>94</sup> Additionally, “lateral” reading (or reading more sources but less in-depth) as defined by Sam Wineburg and Sarah McGrew, emphasizes that people are more likely to believe something is true, even if it contradicts their own opinions, if they are exposed to multiple sources of contrary information instead of simply being told that they are wrong.<sup>95</sup> Ideological nudges, akin to Richard H. Thaler and Cass R. Sunstein’s behavioral economic nudge concept, may therefore help break the extremist cycle by introducing new material and ideas into a digital thought bubble. It may be necessary to consider requiring social media companies to adjust their algorithms to ensure users view a variety of legitimate professional news sources.<sup>96</sup>

Finally, research suggests<sup>97</sup> that the rapid flow of online information discourages rational thinking and favors emotional and heuristic reasoning. Social media companies can decelerate the spread of between mis- and disinformation by slowing down or altering how information is shared on their platforms. Further, functionality could be changed to amplify verifiable information and bury spurious sources. However, social media companies are not incentivized to develop technology to retard information flow, which counters their business model, or to change functionality as changes may push people off their platform. Pressure, if not regulation, from government is required.

Despite the initiatives and efforts discussed above, a major gap remains—no single agency or department is responsible for developing or deploying technology to identify and combat mis- and disinformation. The U.S. government needs to identify a central organization with the mandate of countering mis- and disinformation, developing tools to protect and defend users, and building social information resiliency through coordinated education programs.

## Conclusion

Conventionally understood national security threats do not require the American public or private sector to be actively involved in their management because the Pentagon, the FBI, DHS, and the Intelligence Community are charged to defend the nation and have historically managed national defense and security issues. But, as we have argued in this article, mis- and disinformation, reimagined as a national security threat, are qualitatively different from traditional conceptions of security threats; as the Capitol insurrection laid bare, perhaps they are even more urgent, thus requiring a reordering of U.S. national security priorities. Further, this vulnerable flank is well known to America’s foreign adversaries, and they continue to assault it with seeming impunity.

Because political and civic discourse are increasingly taking place in the information space we have attempted to offer some fruitful avenues of approach for the Biden administration as it crafts its own national security strategy. This is but the tip of the iceberg, however, given the complexity of the challenge. While our recommendations cannot be considered comprehensive in a short article, we emphasize that public, private, and individual aspects are necessary for any truly comprehensive approach.

Despite the instrumental role technology has in amplifying and spreading mis- and disinformation, there is not a technical or government-provided solution to its threat. Instead, it is a whole-of-society threat and *everyone* has a role to play: the private sector, the government, and the public. Understanding and countering the threat of mis- and disinformation is critical to identifying additional interventions to increase the public’s awareness of, and resiliency to, mis- and disinformation. Societal cohesion bolstered by information resiliency is an urgent matter of national security and we urge the Biden Administration to give pride of place in their national security agenda to the complex and urgent threat posed by mis- and disinformation. **PRISM**

## Notes

<sup>1</sup> Craig Kafura, "What Americans Make of the January 6 Chaos at the Capitol", The Chicago Council on Global Affairs, 7 January 2021, <https://www.thechicagocouncil.org/commentary-and-analysis/blogs/what-americans-make-january-6-chaos-capitol>.

<sup>2</sup> Jeffrey M. Berry and Sarah Sobieraj, *The Outrage Industry: Political Opinion Media and the New Incivility*, Reprint Edition (Oxford: Oxford University Press, 2016); Benkler, Faris, and Roberts, *Network Propaganda*.

<sup>3</sup> Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (New York, NY: Oxford University Press, 2018).

<sup>4</sup> Hart, J. & Graether, M. (2018). "Something's going on here: Psychological predictors of belief in conspiracy theories. *Journal of Individual Differences* 39(4): 229-237.

<sup>5</sup> The impact of mis- and disinformation campaigns are not limited to America. For instance, Estonia, Georgia, Ukraine, the Philippines, Britain, and Turkey have all watched as their foundational identities, beliefs, and assumptions about their societies unraveled. See Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War against Reality*, 2019; Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (I.B. Tauris, 2020); Benkler, Faris, and Roberts, *Network Propaganda*.

<sup>6</sup> Conversely, China enforces a policy of tight information control to artificially ensure domestic tranquility and, most importantly, the continued control of the Chinese Communist Party. See Kai Strittmatter, *We Have Been Harmonized: Life in China's Surveillance State* (Custom House, 2020).

<sup>7</sup> "The National Security Strategy of the United States of America", September 2002, accessed at <https://2009-2017.state.gov/documents/organization/63562.pdf>.

<sup>8</sup> "The National Security Strategy of the United States of America", March 2006, accessed at <https://www.comw.org/qdr/fulltext/nss2006.pdf>.

<sup>9</sup> Ibid, p. 10.

<sup>10</sup> "National Security Strategy", February 2015, accessed at [https://obamawhitehouse.archives.gov/sites/default/files/docs/2015\\_national\\_security\\_strategy\\_2.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf).

<sup>11</sup> "National Security Strategy of the United States of America", December 2017, p. 34, accessed at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

<sup>12</sup> "Interim National Security Guidance", March 2021, accessed at <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>.

<sup>13</sup> Ibid, p. 7.

<sup>14</sup> Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, 10 (Penguin UK, 1991), 21.

<sup>15</sup> Robert Bellah et al., *Habits of the Heart: Individualism and Commitment in American Life*, First Edition, With a New Preface edition (University of California Press, 2007).

<sup>16</sup> Gerald Echterhoff and E. Tory Higgins (2018), "Shared reality: Construct and mechanisms", *Current Opinion in Psychology*, pp. 4-6. <https://doi.org/10.1016/j.copsyc.2018.09.003>.

<sup>17</sup> Harriet Martineau, *Society in America Volume 1* (Hard Press, 1837).

<sup>18</sup> Reuben E. Brigety II, "The Fractured Power: How to Overcome Tribalism", *Foreign Affairs*, March/April 2021, accessed at <https://www.foreignaffairs.com/articles/united-states/2021-02-16/fractured-power>.

<sup>19</sup> Brigety II, "The Fractured Power."

<sup>20</sup> Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community*, 1<sup>st</sup> edition (New York, NY: Touchstone Books by Simon & Schuster, 2001).

<sup>21</sup> Bill Bishop and Robert G Cushing, *The Big Sort Why the Clustering of Like-Minded America Is Tearing Us Apart* (Boston, MA: Mariner Books, 2009); Charles A Murray, *Coming Apart: The State of White America, 1960-2010*, 2013.

<sup>22</sup> David V. Gioe, "The Afghanistan Papers and the Perils of Historical Analogy", *Lawfare*, 21 January 2020, accessed at <https://www.lawfareblog.com/afghanistan-papers-and-perils-historical-analogy>.

<sup>23</sup> Patrick Svitek, "Jade Helm 15: The Black Helicopters Are Coming. Well, Maybe Not," *The Texas Tribune*, May 1, 2015, <https://www.texastribune.org/2015/04/30/abbotts-letter-puts-jade-helm-national-stage/>.

<sup>24</sup> Cassandra Pollock and Alex Samuels, "Hysteria over Jade Helm Exercise in Texas Was Fueled by Russians, Former CIA Director Says," *The Texas Tribune*, May 3, 2018, <https://www.texastribune.org/2018/05/03/hysteria-over-jade-helm-exercise-texas-was-fueled-russians-former-cia-/>.

<sup>25</sup> Lane Crothers, *Rage on the Right: The American Militia Movement from Ruby Ridge to Homeland Security*, 0224<sup>th</sup> edition (Lanham, Md: Rowman & Littlefield Publishers, 2003); Jessica Dawson and DB Weinberg, "These Honored Dead: Sacrifice Narratives in the NRA's American Rifleman Magazine," *American Journal of Cultural Sociology*, 2020, <https://doi.org/10.1057/s41290-020-00114-x>; Jessica Dawson, "Shall Not Be Infringed: How the NRA Used Religious Language to Transform the Meaning of the Second Amendment," *Palgrave Communications* 5, no. 1 (July 2, 2019): 58, <https://doi.org/10.1057/s41599-019-0276-z>.



- <sup>26</sup> Jess Walter, *Ruby Ridge: The Truth and Tragedy of the Randy Weaver Family*, Reprint edition (New York: Harper Perennial, 2002); Kenneth S. Stern, *A Force Upon the Plain: The American Militia Movement and the Politics of Hate*, First Edition edition (New York: Simon & Schuster, 1996); Dick Reavis, *Ashes of Waco: An Investigation* (New York: Syracuse University Press, 1998); Kathleen Belew, *Bring the War Home: The White Power Movement and Paramilitary America* (Cambridge, Mass: Harvard University Press, 2018), <http://www.hup.harvard.edu/catalog.php?isbn=9780674286078>.
- <sup>27</sup> Leonard Zeskind, *Blood and Politics: The History of the White Nationalist Movement from the Margins to the Mainstream*, First Edition edition (New York: Farrar, Straus and Giroux, 2009).
- <sup>28</sup> "Assessing Russian Activities and Intentions in Recent US Elections", Director of National Intelligence, 6 January 2017, [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf).
- <sup>29</sup> Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020); Timur Chabuk and Adam Jonas, "Understanding Russian Information Operations", *Signal*, 1 September 2018, accessed at <https://www.afcea.org/content/understanding-russian-information-operations>.
- <sup>30</sup> Philip S. Gorski, *American Covenant: A History of Civil Religion from the Puritans to the Present* (Princeton: Princeton University Press, 2017).
- <sup>31</sup> W. Gardiner Selby, "Doonesbury Says Greg Abbott Activated Texas State Guard in Case of Federal Martial Law and More," @politifact, June 19, 2015, <https://www.politifact.com/texas/statements/2015/jun/19/doonesbury/doonesbury-says-greg-abbott-activated-texas-state-/>. See also Matthew Yglesias, "The amazing Jade Helm conspiracy theory, explained", *Vox*, 6 May 2015, accessed at <https://www.vox.com/2015/5/6/8559577/jade-helm-conspiracy>.
- <sup>32</sup> David V. Goe (2018), "The Cyber operations and useful fools: the approach of Russian hybrid intelligence", *Intelligence and National Security*, 33/7, pp. 954-973. <https://doi.org/10.1080/02684527.2018.1479345>.
- <sup>33</sup> Russia was not the only one who noticed America's social fragility and susceptibility to conspiratorial thinking, domestic fringe movements also took note.
- <sup>34</sup> Elaine Godfrey, "It Was Supposed to Be So Much Worse", *The Atlantic*, 9 January 2021, accessed at <https://www.theatlantic.com/politics/archive/2021/01/trump-rioters-wanted-more-violence-worse/617614/>.
- <sup>35</sup> S. Clarke, "Conspiracy Theories and Conspiracy Theorizing," *Philosophy of the Social Sciences* 32, no. 2 (June 1, 2002): 131-50, <https://doi.org/10.1177/004931032002001>; Michael Barkun, "Conspiracy Theories as Stigmatized Knowledge," *Diogenes*, October 25, 2016, 039219211666928, <https://doi.org/10.1177/0392192116669288>.
- <sup>36</sup> J Hart and M Graether (2018). "Something's going on here: Psychological predictors of belief in conspiracy theories." *Journal of Individual Differences* 39(4): 229-237.
- <sup>37</sup> Kafura, "What Americans Make..."
- <sup>38</sup> Hart and Graether "Something's going on here."
- <sup>39</sup> John Gramlich, "20 Striking Findings from 2020," *Pew Research Center* (blog), December 11, 2020, <https://www.pewresearch.org/fact-tank/2020/12/11/20-striking-findings-from-2020/>.
- <sup>40</sup> Gordon Pennycook et al., "Understanding and Reducing the Spread of Misinformation Online," preprint (PsyArXiv, November 13, 2019), <https://doi.org/10.31234/osf.io/3n9u8>. and what can be done about it? In a first survey experiment (N=1,015).
- <sup>41</sup> Barkun, "Conspiracy Theories as Stigmatized Knowledge."
- <sup>42</sup> Renee DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 9, 2018, <https://yalereview.yale.edu/computational-propaganda>. See also David V. Goe, Michael S. Goodman and Alicia Wanless (2019), "Rebalancing cybersecurity imperatives: patching the social layer", *Journal of Cyber Policy*, 4:1, 117-137, DOI: 10.1080/23738871.2019.1604780, and Daniel Dobrowolski, David V. Goe and Alicia Wanless (2020) "How Threat Actors are Manipulating the British Information Environment", *The RUSI Journal*, 165:3, 22-38, DOI: 10.1080/03071847.2020.1772674.
- <sup>43</sup> Christine Geeng, Savanna Yee, and Franziska Roesner, "Fake News on Facebook and Twitter: Investigating How People (Don't) Investigate," 2020, 14; Karen Hao, "He Got Facebook Hooked on AI. Now He Can't Fix Its Misinformation Addiction," *MIT Technology Review*, March 11, 2021, <https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/>.
- <sup>44</sup> Jessica Dawson, "Microtargeting as Information Warfare," *Cyber Defense Review*, December 7, 2020, <https://doi.org/10.31235/osf.io/5wzuq>.
- <sup>45</sup> Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. government concludes Iran was behind threatening emails sent to Democrats", *Washington Post*, 22 October 2020, accessed at <https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/>.

<sup>46</sup> As quoted in Nakashima, et al.

<sup>47</sup> Mason Clark, "Russian Hybrid Warfare," *Institute For the Study of War*, Military Learning and The Future of War Series, September 2020, <http://www.understanding-war.org/report/russian-hybrid-warfare>.

<sup>48</sup> Doug Livermore, "China's 'Three Warfares' In Theory and Practice in The South China Sea" *Georgetown Security Studies Review*, March 25, 2018, <https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/>.

<sup>49</sup> Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare": The Case of Ukraine," *Center For European Policy Analysis*, January 29, 2021, <https://cepa.org/the-evolution-of-russian-hybrid-warfare-ukraine/>.

<sup>50</sup> Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare": The Case of Ukraine."

<sup>51</sup> Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare": The Case of Ukraine."

<sup>52</sup> Zilvinas Svedkauskas, Chonlawit Sirikupt, and Michel Salzer, "Russia's disinformation campaign are targeting African Americans," *The Washington Post*, July 24, 2020, <https://www.washingtonpost.com/politics/2020/07/24/russias-disinformation-campaigns-are-targeting-african-americans/>.

<sup>53</sup> Elizabeth Grimm Aresnault and Joseph Stabile, "Confronting Russias Role in Transnational White Supremacist Extremism." *Just Security*, February 6, 2020, <https://www.justsecurity.org/68420/confronting-russias-role-in-transnational-white-supremacist-extremism/>.

<sup>54</sup> Natasha Bertrand, "A Model for Civilization: Putin's Russia Emerges As 'A Beacon for Nationalists' and the American Alt-Right", *Business Insider*, December 10, 2016, " <https://www.businessinsider.com/russia-connections-to-the-alt-right-2016-11>.

<sup>55</sup> Natasha Bertrand, "A Model for Civilization."

<sup>56</sup> Alan Ingram, "Alexander Dugin: Geopolitics and neo-fascism in post-Soviet Russia," *Political Geography*, November 2001, Volume 20, Issue 8, <https://www.science-direct.com/science/article/pii/S0962629801000439>.

<sup>57</sup> Doug Livermore, "China's 'Three Warfares.'"

<sup>58</sup> Doug Livermore, "China's 'Three Warfares.'"

<sup>59</sup> David Bowdich, "The Importance of Partnership in Responding to the Chinese Economic Espionage Threat to Academia" *Academic Security and Counter Exploitation Annual Seminar*, Texas A&M University, March, 4 2020 <https://www.fbi.gov/news/speeches/the-importance-of-partnerships-in-responding-to-the-chinese-economic-espionage-threat-to-academia>.

<sup>60</sup> Johan Blank, "China Bends Another American Institution to Its Will," *The Atlantic*, October 10, 2019, <https://www.the-atlantic.com/international/archive/2019/10/nba-victim-china-economic-might/599773/>.

<sup>61</sup> Douglas Larson, "China's Emerging Soft Power Strategy in Hollywood," *Naval Postgraduate School*, September 2019, <https://www.hsdll.org/?view&did=831031>.

<sup>62</sup> Jeffrey Mervis, "'Has it Peaked? I don't know.' NIH officials details foreign influence probed." *Science Magazine*, June 22, 2020, <https://www.sciencemag.org/news/2020/06/has-it-peaked-i-don-t-know-nih-official-details-foreign-influence-probe>.

<sup>63</sup> Johan Blank, "China Bends Another American Institution to Its Will."

<sup>64</sup> Zack Beauchamp, "One of America's Biggest Game Companies is acting as a Chinese Censor," *Vox*, October 8, 2019, <https://www.vox.com/2019/10/8/20904433/blizzard-hong-kong-hearthstone-blitzchung>.

<sup>65</sup> Douglas Larson, "China's Emerging Soft Power Strategy in Hollywood."

<sup>66</sup> Elizabeth Chen, "Chinese COVID-19 Misinformation a Year Later," *The Jamestown Foundation*, February 4, 2021, <https://jamestown.org/program/chinese-covid-19-misinformation-a-year-later/>.

<sup>67</sup> Jon Bateman and Craig Newmark, "Social Media Disinformation Discussions Are Going in Circles. Here's How to Change That", *Slate*, 24 March 2021, <https://slate.com/technology/2021/03/online-disinformation-congressional-hearing-amazon-google-twitter-ceos.html>.

<sup>68</sup> Yoel Roth and Nick Pickels, "Updating our approach to misleading information," *Twitter*, May 11, 2020, [https://blog.twitter.com/en\\_us/topics/product/2020/updating-our-approach-to-misleading-information.html](https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html).

<sup>69</sup> Savvas Zannettou, "I Won the Election! An Empirical Analysis of Soft Moderation Interventions on Twitter," *Cornell University ArXiv* January 18, 2021, <https://arxiv.org/abs/2101.07183>.

<sup>70</sup> Ben Collins and Brandy Zanzrozy, "Reddit Bans Qanon Subreddit after months of violent threats," *NBC News*, September 12, 2018, <https://www.nbcnews.com/tech/tech-news/reddit-bans-qanon-subreddits-after-months-violent-threats-n909061>.

<sup>71</sup> Manoel Horta Ribeiro et al, "Does Platform Migration Compromise Content Moderation," *Cornell University Arxiv*, October 21, 2020, <https://arxiv.org/abs/2010.10397>.

<sup>72</sup> David V. Goe, "The History of Fake News", *The National Interest*, 1 July 2017, <https://nationalinterest.org/feature/the-history-fake-news-21386>.

<sup>73</sup> Arielle Pardes, "Parler Games: Inside the Right's Favorite 'Free Speech' App," *Wired Magazine*, November 12, 2020, <https://www.wired.com/story/parler-app-free-speech-influencers/>.

<sup>74</sup> Joseph Littell, "Don't Believe Your Eyes or Ears: The Weaponization of Artificial Intelligence, Machine Learning, and Deepfakes," *War on the Rocks*, October 7, 2019, <https://warontherocks.com/2019/10/dont-believe-your-eyes-or-ears-the-weaponization-of-artificial-intelligence-machine-learning-and-deepfakes/>.

<sup>75</sup> Associated Press, "Cheerleader's mom accused of making 'deepfakes' of rivals," *Associated Press News*, March 15, 2021, <https://apnews.com/article/pennsylvania-doylestown-cheerleading-0953a60ab3e-3452b87753e81e0e77d7f>.

<sup>76</sup> Kevin Roose, "The Making of a YouTube Radical," *The New York Times*, 8 June 2019, <https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html>.

<sup>77</sup> Hao, "He Got Facebook Hooked on AI. Now He Can't Fix Its Misinformation Addiction."

<sup>78</sup> Ibid.

<sup>79</sup> Barkun, "Conspiracy Theories as Stigmatized Knowledge"; Clarke, "Conspiracy Theories and Conspiracy Theorizing."

<sup>80</sup> Karsten Muller and Carlo Schwarz. (2018). "Fanning the Flames of Hate: Social Media and Hate Crime." *Centre for Competitive Advantage in the Global Economy*.

<sup>81</sup> Dana Weinberg and Jessica Dawson, "From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity," *Brookings*, 2021, <https://doi.org/10.31235/osf.io/87zmk>.

<sup>82</sup> Zeynep Tufekci, "View of Engineering the Public: Big Data, Surveillance and Computational Politics | First Monday," *First Monday* 19, no. 7 (2014), <https://firstmonday.org/ojs/index.php/fm/article/view/4901/4097>.

<sup>83</sup> Gabriele Cosentino, *Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation* (Cham: Springer International Publishing, 2020), <https://doi.org/10.1007/978-3-030-43005-4>.

<sup>84</sup> Renee Diresta and Tobias Rose-Stockwell, "How to Stop Misinformation Before It Gets Shared," *Wired*, March 26, 2021, <https://www.wired.com/story/how-to-stop-misinformation-before-it-gets-shared/>.

<sup>85</sup> Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, <https://doi.org/10.1126/science.aap9559>.

<sup>86</sup> DiResta, "Computational Propaganda: If You Make It Trend, You Make It True."

<sup>87</sup> Saara Salomaa and Lauri Palsa, "Media Literacy in Finland: National Media Education Policy," *Publications of the Ministry of Education and Culture*, 2019, <https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf>.

<sup>88</sup> Intelligence Unit, "Democracy Index 2018: Me too? Political Participation, Protest and Democracy" *The Economist*, 2018, [https://www.eiu.com/public/topical\\_report.aspx?campaignid=democracy2018](https://www.eiu.com/public/topical_report.aspx?campaignid=democracy2018).

<sup>89</sup> Nic Newman et al, "Reuters Institute Digital News Report 2018," *Reuters Institute for the Study of Journalism*, 2018, <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/digital-news-report-2018.pdf>.

<sup>90</sup> Samar Ali, "Millions of Conversations," <https://millionsofconversations.com/team.html>.

<sup>91</sup> Cybersecurity and Infrastructure Security Agency, "#Protect 2020: Rumor Vs. Reality," <https://www.cisa.gov/rumorcontrol>.

<sup>92</sup> Christopher Krebs "Opinion: Trump fired me for saying this, but I will say it again: The election wasn't rigged," *The Washington Post*, December 1, 2020, [https://www.washingtonpost.com/opinions/christopher-krebs-trump-election-wasnt-hacked/2020/12/01/88da94a0-340f-11eb-8d38-6aea1adb3839\\_story.html](https://www.washingtonpost.com/opinions/christopher-krebs-trump-election-wasnt-hacked/2020/12/01/88da94a0-340f-11eb-8d38-6aea1adb3839_story.html).

<sup>93</sup> David Gioe, "The History of Fake News," *The National Interest*, July 1, 2017, <https://nationalinterest.org/feature/the-history-fake-news-21386>.

<sup>94</sup> Benkler, Faris, and Roberts, *Network Propaganda*.

<sup>95</sup> Sam Wineburg and Sarah McGrew, "Lateral Reading: Reading Less and Learning More When Evaluating Digital Information," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, October 6, 2017).

<sup>96</sup> We acknowledge the difficulty in securing universal agreement on what constitutes "legitimate" news sites.

<sup>97</sup> Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," *Oxford Handbook of Cyber Security*, August 11, 2017, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3015680](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680).